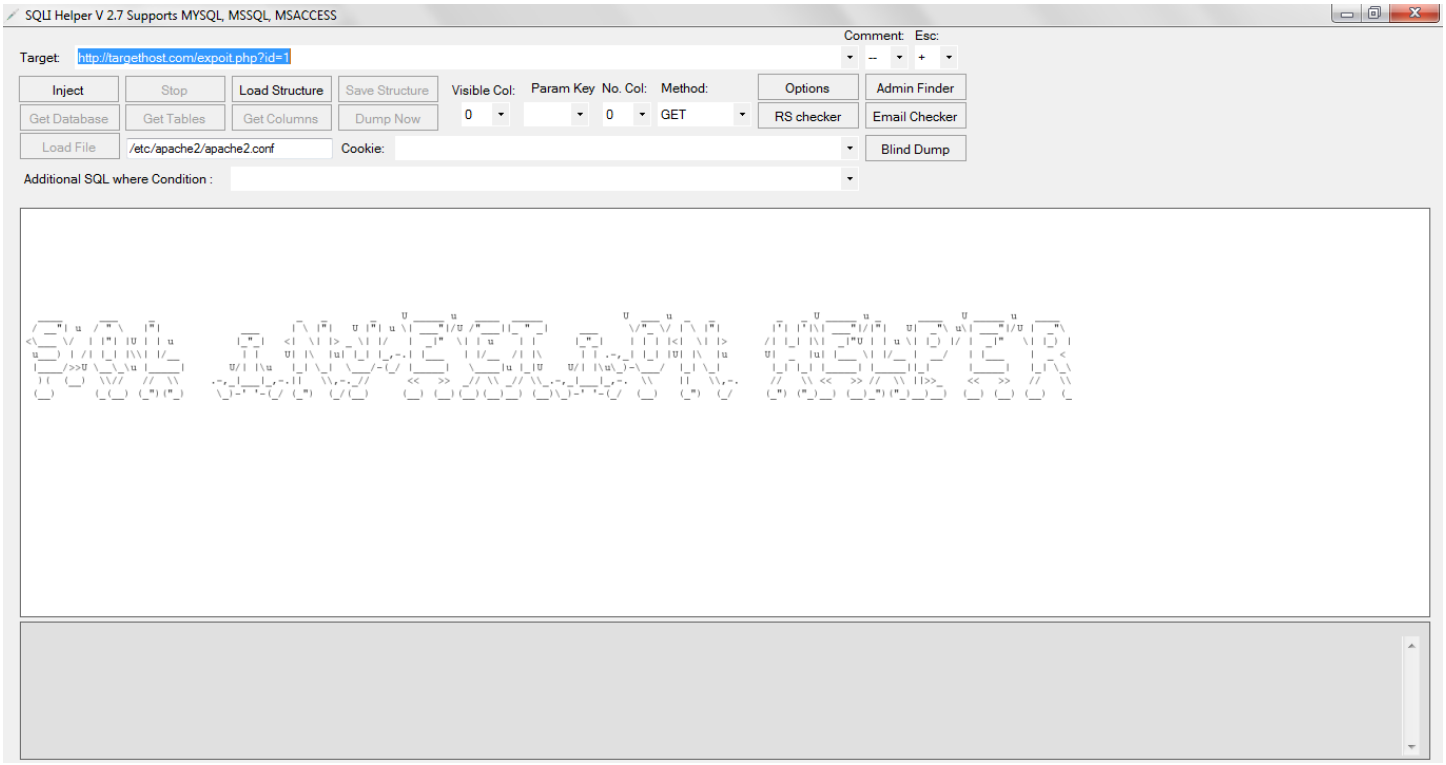
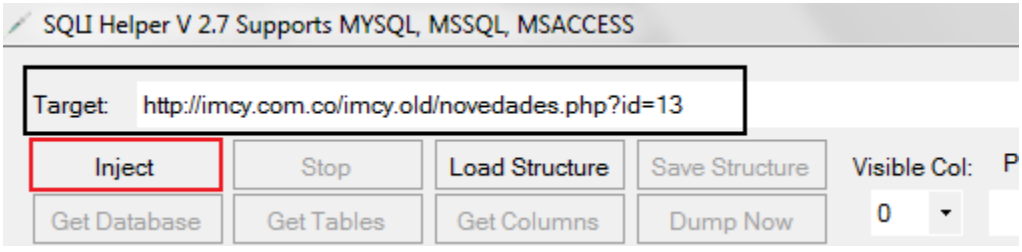
Pasos para manejar SQL Helper

Al ejecutar SQL Helper, nos encontraremos con esta ventana inicial. Este manual explicara los botones que nos ayudaran a verificar si nuestra aplicación tiene alguna vulnerabilidad.

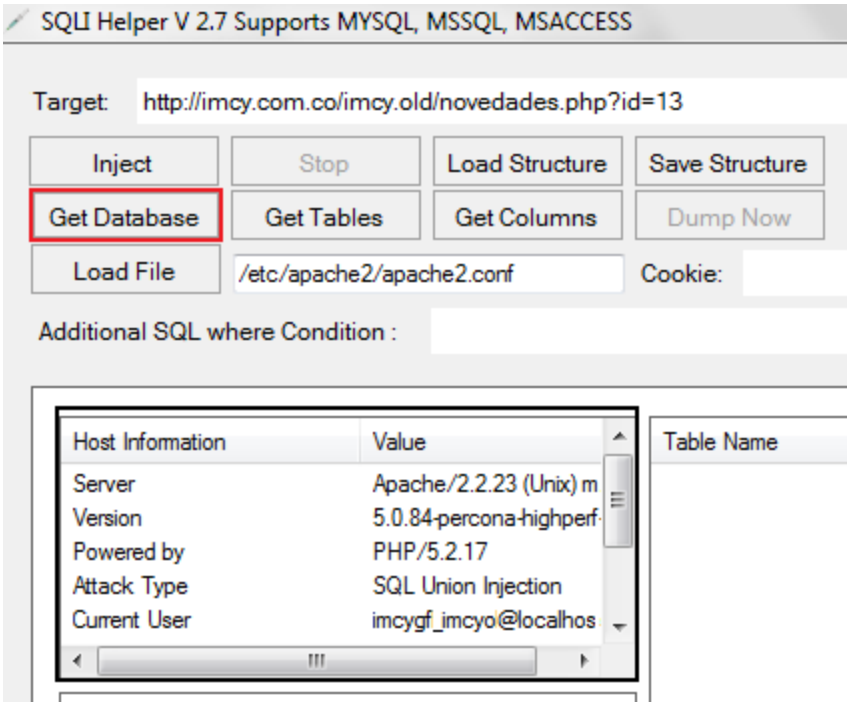


1. Tomar la URL de la página: Usted deberá copiar el enlace la página a la cual quiere verificarle si tiene alguna vulnerabilidad. El enlace ya anteriormente copiado se pegara en la casilla “Target” de SQL Helper (Rectángulo Negro) y seguidamente damos clic en el botón “Inject” (Rectangulo Rojo):



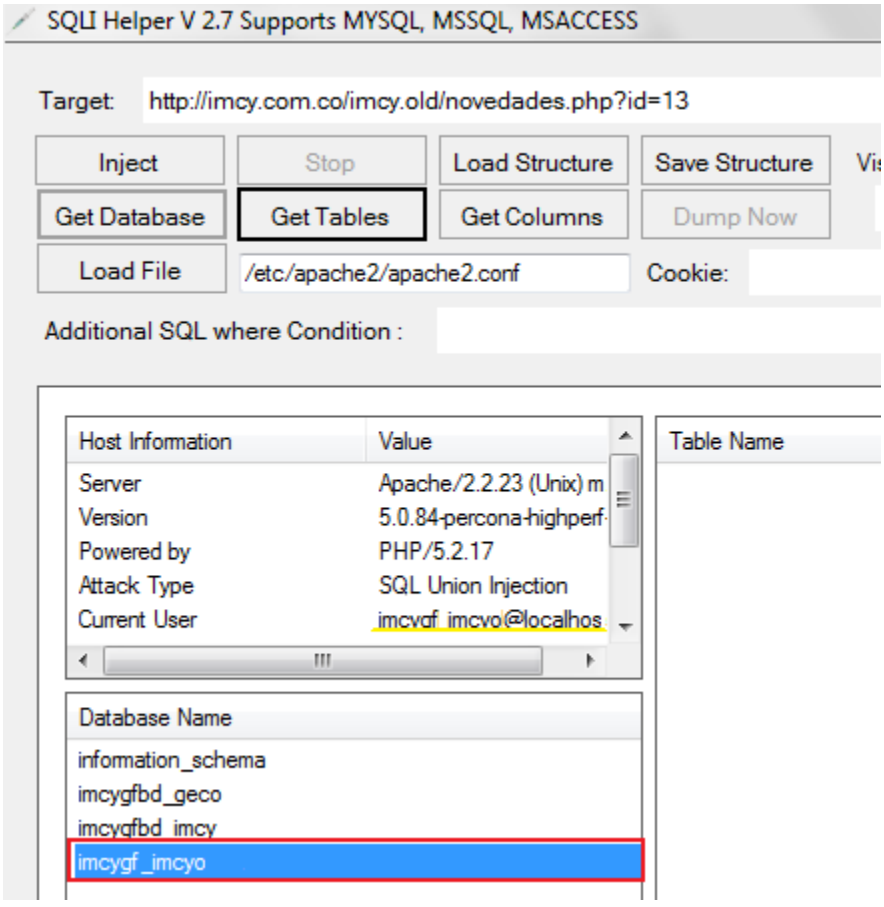
2. Obtener Base de Datos de la Página: Se desplegara la siguiente información, la cual nos va a ser útil para verificar la base de datos que contiene todos los datos deseados (Para este caso Usuario y Contraseña).

Luego que obtenemos la información de la inyección (Rectángulo Negro), vamos a oprimir el botón “Get Database” (Rectángulo Rojo) para obtener el nombre de la base de datos con que trabaja esa página.

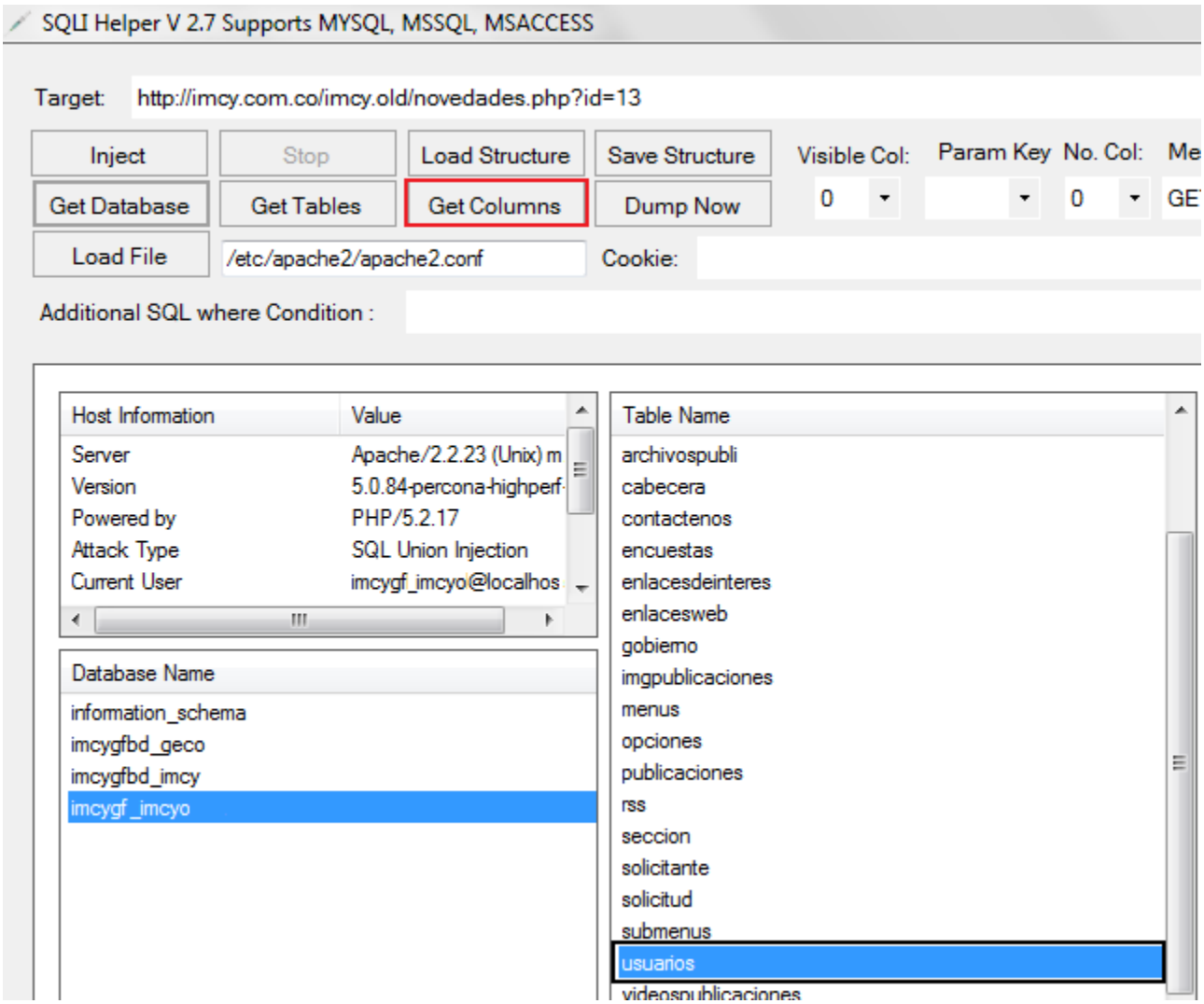


3. Obtener Tablas a Partir del Nombre de la Base de Datos: Para obtener las tablas y las columnas de esa página específica, debemos tener en cuenta el verdadero nombre de la base de datos. Entonces seleccionaremos "imcygf_imcyo" (Rectángulo Rojo) que es el mismo nombre que se obtiene cuando damos clic en "Injection" (Línea Amarilla), pues el programa puede mostrar información adicional que por el momento no será de mucha utilidad.

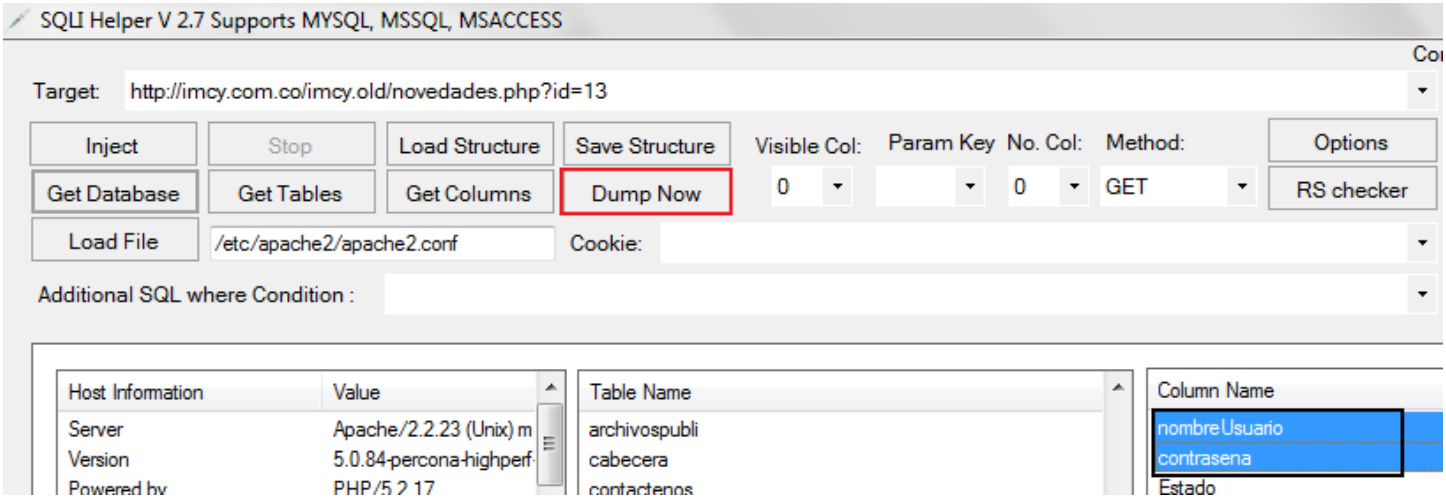
Para obtener las tablas de esa base de datos, damos clic en "Get Tables" (Rectángulo Negro).



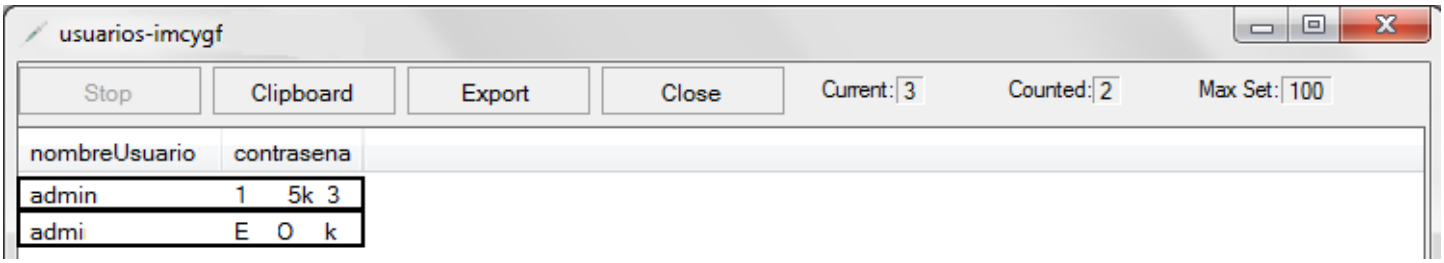
4. Obtener Columnas a partir de la Tabla Seleccionada: Luego de obtener las tablas de la base de datos, debemos seleccionar la tabla que más no llame la atención o a la cual le queremos sacar información. En nuestro ejemplo tomaremos la llamada “Usuarios” (Rectángulo Negro) y luego damos clic en el botón “Get Columns” (Rectángulo Rojo). Recuerda que solo mostrara las columnas de esa tabla en específico.



5. Revisar los Registro de la Columna: En nuestro ejemplo solo seleccionaremos dos columnas, “nombreUsuario” y “contrasena” (Rectángulo Negro), pues es la información que nos interesa saber. Para obtener la información de esas columnas damos clic en el boton “Dump Now”:



Si se han realizado todos los pasos correctamente, obtenemos la siguiente ventana que contiene los registros de la base de datos de la tabla Usuarios.



NOTA: Por respeto al compañero que presto su pagina para verificar la vulnerabilidad de esta, no se ha publicado el link que contiene la vulnerabilidad, la información de su base de datos, ni los registros. Si usted quiere probar con otra página en el manual de instalación de SQL Helper se encuentra el nombre de un archivo con páginas vulnerables.